AMENDMENTS TO THE SPECIFICATION

Please amend page 7 of the specification, at the carryover paragraph, as follows:

injection or patching to inject logic into one or more modules 1,15 within database server 2, to transfer control to training module 4. In another embodiment, called "direct database integration", the database 1 vendor, who has access to the commands 5 in conjunction with the normal operation of the database[[5]] 1, makes the commands 5 available to intrusion detection system 19. In yet another embodiment, in cases where database 1 supports it, external database log file 12 may be examined without the need to resort to special software. Once an event has been processed by the IDS 19, it can optionally be expunged from any table or log file it is stored in, to make room for subsequent events.

Please also amend page 6 of the specification, at the last paragraph, as follows:

The event data can appear in string or binary form, and can be extracted using a number of different techniques, depending on the implementation of the IDS 19, including APIs (Application Programming Interfaces) that access the computer code 1. One example is to use ODBC (Open DataBase Connectivity), a set of C language API's that allows one to examine or modify data within database 1. If the ~~Java~~ JAVA programming language is used, JDBC (~~Java~~ JAVA DataBase Connectivity) can be used instead. Another way of extracting the needed information from database 1 is to use code injection or patching to inject logic into one or more modules 1,15 within database server 2, to transfer control to training module 4.